МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ
Кафедра высшей алгебры и защиты информации

РУБИНА
Ксения Дмитриевна

Аннотация к дипломной работе «Полиномиальный детерминированныйалгоритм тестирования на простоту»

Научный руководитель:
доцент, кандидат физико-математических наук,
Д. В. Васильев

Минск, 2014

Дипломная работа состоит из 4 глав, введения и заключения общим объемом 31 страница; содержит 4 графика, 19 источников.

Ключевые слова: ПРОСТОЕ ЧИСЛО, СОСТАВНОЕ ЧИСЛО, ПОРЯДОК, ВЫЧЕТ, МОДУЛЬ, СРАВНЕНИЕ, СЛОЖНОСТЬ АЛГОРИТМА.

В дипломной работе изучается полиномиальный детерминированныйалгоритм тестирования на простоту.

Целью дипломной работыявляется исследование алгоритма AKS, его обоснований, получение его программной реализации. Также был проведен обзор детерминированных и вероятностных алгоритмов тестирования на простоту.

В дипломной работе были изучены следующие алгоритмы:

- вероятностные алгоритмы с односторонней ошибкой (тест Лемана, тест Соловея-Штрассена, тест Миллера-Рабина, QFT);
- алгоритмы с вероятностным временем выполнения (ECPP, SEA);
- детерминированные алгоритмы(решето Эратосфена, алгоритм пробного деления, APR).

В дипломной работе получены следующие результаты:

- исследованы основания алгоритма AKS;
- доказана теорема AKS;
- оценена сложность алгоритма;
- получена программная реализация.

Belarusian State University

Faculty of Mechanics and Mathematics

Department of Higher Algebra and Information Security

Abstract for diploma paper

Polynomial deterministic algorithms for primality testing

Rubina Kseniya Dmitrievna

Supervisor

Denis Vladimirovich Vasiliev

2014

Diploma work consists of4 chapters, introduction and conclusion, contains 31 pages, 4graphics, 19 sources.

Key words: PRIME NUMBER, COMPOSITE NUMBER, ORDER, RESIDUE, MODULE, CONGRUENCE RELATION, COMPLEXITY OF ALGORITHMS.

In the diploma work we studied a polynomial deterministic algorithm for testing primality.

The aim of the thesis is the investigation of the AKS algorithm, its proofs, getting its program implementation. Also wereviewed the deterministic and randomized algorithms for testing primality.

In the diploma work we studied the following algorithms:

- randomized algorithms with one-sided error (Lehmann, Solovay-Strassen, Miller-Rabin, QFT);
- algorithms with randomized execution time (ECPP, SEA);
- deterministic algorithms (the sieve of Eratosthenes, trial division, APR).

In the diploma work we obtained the following results:

- the grounds of AKS algorithm were studied;
- the AKS theorem was proved;
- the complexity of the algorithm was estimated;
- program implementation was received.